ETHICAL GUIDELINES FOR BLOCKCHAIN SYSTEMS

Complete Research

Signe Agerskov, IT University of Copenhagen, Copenhagen, Denmark, sigm@itu.dk

Asger Balle Pedersen, IT University of Copenhagen, Copenhagen, Denmark, asbp@itu.dk

Roman Beck, IT University of Copenhagen, Copenhagen, Denmark, romb@itu.dk

Abstract

Enterprise architects and IT systems developers must often decide ad hoc how to identify, assess and mitigate ethical issues of autonomous, rule-based systems based on blockchain technology. As blockchain systems are decentralized and immutable, developers must assess ethical risks, not only on an individual level but also on a network level along the life-cycle stages of a blockchain system. These ethical issues should be addressed and ideally mitigated by clearly defined norms and values that are intentionally incorporated in a blockchain system. As a reference for a normative system, we have chosen the European Union and its ethical values to discuss them in the context of ethical issues emerging from blockchain systems. This paper presents a top-down approach that establishes ethical guidelines for blockchain systems based on ethical issues mapped against European values.

Keywords: Ethics, Blockchain, Guidelines, Information Systems.

1 Introduction

As the digital transformation of all parts of society continues, technology has become an integral part of all areas of public and private life. Technology is no longer just an add-on that organizations use to gain competitive advantages but is an endogenous part of economic and societal activities alike (Vial, 2019). With the emergence of disruptive technologies such as blockchain technology, artificial intelligence (AI), and the internet of things (IoT), the next digital transformation will be characterized by moving from reactive automatic systems to proactive autonomous ones (Beck et al., 2022). In blockchain systems, code can be executed autonomously when predefined conditions are met; for example, when transaction-based, append-only databases distributed in a peer-to-peer network execute business logic via the use of so-called smart contracts (Beck et al., 2017). Once smart contracts are deployed on a blockchain system they become an autonomous actor within their designed and implemented parameters. Thus, a blockchain-based application using a smart contract can be considered a kind of independent agent, acting on values and principles encoded in the system to ensure safe and reliable transactions (Moor, 2020).

Having autonomous non-human actors interacting with human agents and organizational entities can create ethical issues and conflicts, as these actors operate according to predefined rules and are incapable of adjusting to specific situations. If they are embedded in back-end transactions, they can create unforeseen social consequences (Tang et al., 2019a). In particular, when public services are based on blockchain systems, it is important to ensure that the encoded values and norms are in line with social values. An example is the European Blockchain Services Infrastructure (EBSI) which is currently under development to become the backbone for cross-border transactions within the European Union (EU). Autonomous systems should ideally be subject to some sort of ethical risk assessment (Winfield, 2019) to ensure that predefined settings of autonomous actors are ethically sound and based on commonly understood and socially accepted norms (Anderson and Anderson, 2020)

Ethics in brief describe norms of "right and wrong" that are based on human reasoning and logic (Lapointe and Fishbane, 2019). Ethics can be applied as principles, based on ideas of fairness, rights, virtues, societal benefit, and obligations, that prescribe how to act in specific circumstances, and sometimes are codified into frameworks designed to support individual decision-making (Fischer, 2018; Tang et al., 2019b). In the realm of technology, ethical considerations have been identified and assessed for AI (European Commission, 2019a), IoT (Baldini et al., 2016), and human-computer interaction (HCI) (Friedman and Kahn, 2002), but the discussion of ethics in the context of blockchain is still in its infancy (Kučera and Bruckner, 2019). Given blockchain's status as a fundamental infrastructure that might become part of the internet itself (Nofer et al., 2017), a broader discourse on the ethical implications of blockchain-based autonomous systems is overdue. But in the absence of clear ethical guidelines for blockchain systems, it is up to enterprise architects and IT systems developers to identify, assess, and mitigate the risks of autonomous, rule-based systems. This is a bottom-up approach to deriving morally acceptable ways for subsystems and users to interact (Wallach et al., 2020). To prevent ethical harm arising from poorly considered design or inappropriate implementation, ethical reflections in information systems (IS) must consider all stages in the life cycle of a blockchain system before it is put into production (Winfield et al., 2019). In this research, we will answer the following question within IS field: *How should ethical guidelines be developed for blockchain system in relation to EU values?*

2 Research methodology

In order to address the research question, we conducted a literature review inspired by the works of Webster and Watson (2002) to identify ethical blockchain issues discussed in prior research within the IS field. We then conducted an in-depth case investigation to identify European values in order to assess the ethical issues related to blockchain and create ethical guidelines for blockchain systems (Wynn Jr and Williams, 2012; Yin, 2003).

To identify ethical issues, we used a search string (ethic* AND blockchain) that concluded with 336 articles in the Association for Information Systems (AIS) eLibrary before assessing the papers. First, we only included peer-reviewed articles from 2008 onwards, which reduced the number of articles to 76. Second, we then analysed the 76 articles to identify which ethical issues arise in the design and development of blockchain systems. Third, we extracted the ethical issues from the articles and ran them through an iterative process among the authors to identify similarities (Ryan and Bernard, 2003), which reduced the scope to 25 IS articles. Fourth, based on the analysis of ethical issues from the 25 IS articles, we further identified non-IS papers relevant to this research, which we included for the sake of completeness. The final scope of articles relevant to this research was 40 and listed in table 1. Each ethical theme was based on the underlying issues from the 40 articles and is described in detail in section 4.

We also needed to establish which principles and values should be considered in the design and development of a blockchain system. Hence, we conducted an in-depth case investigation of European values, inspired by Yin (2003), based on statements from European Commission and Connecting Europe Facility (CEF) for EBSI standards. The collected data was than analysed and discussed by all authors to triangulate the perspectives (Miles and Hubermann 1994) in identifying ethical issues around EBSI. Our data collection also included EU directives and declarations as well as academic literature defining and conceptualizing EU values. All data was analysed and coded by the three authors. Subsequently, categories were developed in an iterative process by the authors where discrepancies and commonalities were discussed. This research approach to analyse ethical blockchain design and –development allowed us to define ethical principles and values that developers should consider (Wallach et al., 2020).

3 Ethical research in information systems

As information technology became an inseparable part of society, it is necessary to consider emerging ethical implications, as unforeseen and unintended consequences with severe impact on society may emerge (Moor, 1985). Hirschheim and Heinz (1994) point out that IS scholars have favoured research on efficiency and cost aspects of IS over social and ethical implications, which in consequence may have led to a reproduction and empowerment of existing structures, as well as social inequalities. However, some ethical considerations have been discussed also in prior IS research, including normative beliefs, the ethical climate of organizations, and organizational scenarios involving ethical issues (Leonard and Cronan, 2001). Often, IS research on ethics is focused on the individual level: that is, the user of information technology (IT) or the IS professional tasked with developing or implementing systems (Couger, 1989; Johnson, 2004; Oz, 1992). Such research considers situations where individuals must make an ethical decision (Leonard and Cronan, 2001). IS research has also considered ethical behaviour in design science research, in particular how to implement ethical guidelines in designing new information systems (Benke et al., 2020). Myers and Venable (2014) have summarized the ethical challenges that can materialize in design science in terms of six principles: (1) consider the public interest, (2) obtain informed consent, (3) protect privacy, (4) create honest and accurate artefacts, (5) ensure that intellectual property rights are met, and finally, (6) ensure high quality of the IT artefact.

In more recent IS research on ethics, challenges emerging from AI (Vakkuri and Abrahamsson, 2018) and big data analytics (Richardson et al., 2021) have been at the centre of interest. This research emphasizes that prescribing recommendations such as ethical guidelines requires both a fine-grained understanding and caution. To our knowledge, how developers and users employ ethical values, as well as the potential ethical consequences of blockchain systems on a societal level, have not yet been researched.

Current IS research on ethics predominantly focuses on the individual level as well as on the design and use of IT artefacts. So far, research has not considered that developers might not be uniquely identifiable nor that it can be unclear who are the users, which can be the case with blockchain systems. Decisions made in the design and development phase of a blockchain system can later cause ethical consequences for the whole network. However, protocol and smart contract developers might not be aware of the consequences they create for the network at a later stage. This intertwined relationship between individual decision-making and the ethical effects on a network level has not been studied in depth so far.

4 Ethical issues in blockchain systems

With the emergence and evolution of blockchain systems, new actions and business models became possible. Blockchain technology enables decentralized systems and the network-based provisioning of public goods, with no need for a trusted third party (for example, Bitcoin, which is not controlled by any government). As blockchain has the potential to influence or change fundamental structures in society, it is important to establish norms, morals, or rules for how blockchain systems are governed. This section identifies ethical issues related to blockchain systems and is intended to serve as a foundation for establishing ethical guidelines. The following table show an overview of the ethical issues identified in the literature review (see table 1).

Ethical issues	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**
Alshamsi and Andras (2019, p.95–97, 106)						x	
Ar et al. (2020, p.1, 6–9)		x					x
Bamakan et al. (2020, p.2–4, 9, 18)	x			x			
Beck et al. (2018, p.6, 28, 35–36)	x				x		x
Beck et al. (2022, p.266, 271)			x				

Calvaresi et al. (2019, p.379-380)		x				x	
Chang et al. (2020, p.2–5)		x	x	x	x	x	x
Dierksmeier and Seele (2018, p.5, 7–11)						x	
Dierksmeier and Seele (2020, p.351–355)			x				
Drobyazko et al. (2019, p.3–4)						x	x
DuPont (2019, p.5, 13–15)							x
Ehrenberg and King (2020, p.33–34)							x
Ertemel (2018, p.44)	x						
Farrugia et al. (2020, p.2–3)					x		x
Fischer (2018, p.1, 4–8)		x		x	x		x
French et al. (2021, p.10)		x				x	
Gomber et al. (2018, p.242–246)							x
Hacioglu et al. (2021, p.3, 9)				x			
Ingold and Langer (2021, p.2–3)		x			x		
Ingram Bogusz and Morisse (2018, p.1189)					x		
Ishmaev (2020, p.1–2, 6)			x			x	
Jørgensen and Beck (2022, p.1-2, 8)					x	x	
Kaygın et al. (2018, p.188)				x			
Kučera and Bruckner (2019, p.132–133, 137)		x	x				
Lapointe and Fishbane (2019, p.58–63, 66–68)			x	x	x	x	
Li and Whinston (2020, p.21)		x			x		
Migliorini et al. (2019, p.2)		x					x
Ølnes et al. (2017, p.355, 360)		x	x		x		
Palas and Bunduchi (2020, p.474)		x					
Parkhomenko et al. (2019, p.3–4)				x			x
Perdana et al. (2021, p.12)							x
Qureshi et al. (2021, p.6–7, 25)		x					
Rana et al. (2021, p.554, 564)		x					x
Rossi et al. (2019, p.1392-1393, 1396, 1400)						x	
Scholl and Bolivar (2019, p.601, 608)					x	x	
Sun Yin et al. (2019, p.39, 65–67)						x	
Tang et al. (2019a, p.45–48)			x		x	x	
Tang et al. (2019b, p.605–606, 610, 619–624)		x	x		x		
Toufaily et al. (2021, p.2, 4–6)		x			x	x	
Zachariadis et al. (2019, p.112–115)					x		

Table 1. Ethical Issues from Blockchain Literature.

4.1 Supreme power by design (I1)

As noted earlier, blockchain systems are transaction-based, append-only databases distributed in a peer-to-peer network. The distributed network uses a consensus algorithm to achieve decentralization. The term “consensus” refers to the interactions between entities, where, for example, governance is dispersed or delegated away from a single central entity (Beck et al., 2018). Decentralization allows for distributed power, which can be preferred to having a single authority potentially acting in its own best interests (Bamakan et al., 2020). However, some blockchain-based designs and implementations

are not fully decentralized but place the majority of the decision power in the hands of a few. This means that blockchain systems also can be designed and used in ways that cement or even enhance the power of centralized authorities (Ertemel, 2018).

4.2 Exclusion and privacy (I2)

Exclusion from blockchain systems may take place on an organizational or individual level. Entities governing a blockchain system may monopolize a network in a market or industry, as they can control who can participate and hereby can make it challenging for stakeholders to conduct business if excluded (Fischer, 2018; Palas and Bunduchi, 2020). On an individual level, blockchain systems could unintentionally designed to exclude users if limitations such as computational literacy, physical abilities, and access to hardware are not considered (Lapointe and Fishbane, 2019). Once entities are part of the network, recording and storing data on blockchains ensures data integrity among all peers via the distributed consensus. This makes the data and transactions both quasi-immutable and transparent for each peer (Chowdhury et al., 2018). Transparency is generally considered to be positive; however, in the context of sensitive data, it may be preferable to handle data confidentially and to be able to delete such data if necessary. As data in a blockchain system cannot be deleted, it may be impossible to enforce something like the General Data Protection Regulation (GDPR) and the "right to be forgotten" (Calvaresi et al., 2019; French et al., 2021; Ingold and Langer, 2021; Kučera and Bruckner, 2019; Lapointe and Fishbane, 2019; Li and Whinston, 2020; Migliorini et al., 2019; Rana et al., 2021; Toufaily et al., 2021; Qureshi et al., 2021; Ølnes et al., 2017).

4.3 Unforeseen consequences of codification (I3)

Blockchain systems enable the execution and deployment of smart contracts. We consider these to be a kind of "ethical agent" that acts and triggers incentives, stimulating a certain behaviour in the blockchain network (Moor, 2020). These ethical agents enable new types of organizations, such as decentralized autonomous organizations (DAOs) which could codify universal rules, values, and norms causing either positive or negative social impact (Beck et al., 2022; Ishmaev, 2020; Kučera and Bruckner, 2019; Lapointe and Fishbane, 2019; Tang et al., 2019b; Ølnes et al., 2017). An example where delegating decision rights to smart contracts happened at the expense of human dignity is Augur: Augur is a DAO-based prediction market that allows anonymous betting. However, when people started betting on when famous individuals would pass away, it turned into a potential assassination market by essentially creating an incentive to kill those individuals in order to receive the money (Dierksmeier and Seele, 2020)

4.4 Depletion of resources (I4)

The consensus algorithm used to govern a blockchain also dictates and influences the security and sustainability of the network (Bano et al., 2017). The highest security, which comes from the proof of work (PoW) algorithm, has the disadvantage that the validation of blocks requires a lot of electricity (Bamakan et al., 2020; Fischer, 2018; Hacioglu et al., 2021; Kaygın et al., 2018; Lapointe and Fishbane, 2019; Parkhomenko et al., 2019). The Bitcoin blockchain network alone consumes more than 90 terawatts per year (Chang et al., 2020). This makes some blockchain systems consume vast amounts of energy.

4.5 System threats (I5)

Other consensus algorithms, like proof of stake (PoS), use less energy, but present other trade-offs. For example, a blockchain system using the PoW consensus protocol is more secure, as more than 50 per cent of the network must be compromised before an attack is possible, whereas the PoS protocol is vulnerable at 34 per cent (Chang et al., 2020; Li and Whinston, 2020; Toufaily et al., 2021). Another threat to systems is hard forks where a blockchain ledger is divided into two branches. In the case of

the 2016 scandal at the venture capital fund The DAO, money was stolen but recovered by making a hard fork revoking the history of events. (Chang et al., 2020; Fischer, 2018; Li and Whinston, 2020; Tang et al., 2019a; Toufaily et al., 2021). This ultimately challenges the purpose of an immutable ledger and a single shared truth, as one ledger is branched into two creating more than one version of the ledger. The entire scandal at The DAO was made possible due to a programming weakness in the smart contracts, even though several code reviews were conducted before implementation (Farrugia et al., 2020; Rossi et al., 2019). Fraud is also categorized as a security concern, as scammers could exploit the lack of knowledge or create a middleman attack pretending to be someone else (Ingold and Langer, 2021; Toufaily et al., 2021). Lastly, wallet keys can compose a threat if not stored securely. Every transaction and data transformation in the network has an identifier key, which is signed by a wallet telling where it originated from (Jørgensen and Beck, 2022; Tosh et al., 2017, Ølnes et al., 2017). If the (private) wallet key is lost, there are no options for retrieval, and the wallet assets and funds will be frozen indefinitely (Aydar et al., 2019). In November 2017 a GitHub user accidentally lost the wallet key to approximately 500,000 Ethereum (ETH), which made it nearly impossible to retrieve the ETH afterwards (Zachariadis et al., 2019). The potential for devastating consequences is clear, for example an elderly person losing the key to his or her entire life savings.

4.6 Lax accountability (I6)

Having every transaction signed in a network ensures data provenance, but it does not automatically add accountability to the system. Accountability depends on the design of the network, whether it is public or private, and whether it allows individuals to join and create a self-sovereign identity anonymously or by registration (Beck et al., 2018; Calvaresi et al., 2019; Ishmaev, 2020; Jørgensen and Beck, 2022; Lapointe and Fishbane, 2019; Tang et al., 2019a). When creating a new account in a conventional bank, it is mandatory for the bank to run a Know Your Customer (KYC) check, but in a blockchain system (for example, Bitcoin) users can set up a wallet in seconds (Alshamsi and Andras, 2019; French et al., 2021; Toufaily et al. 2021). Without a background check, it is easier for people with malicious intent to join the network. They might want to use the blockchain system for money laundering or tax evasion or to use cryptocurrencies for drug and weapons payments (Dierksmeier and Seele, 2018; Farrugia et al., 2020; Gomber et al., 2018; Scholl and Bolivar, 2019; Sun Yin et al., 2019). Lastly, smart contracts in blockchain systems can facilitate autonomous executions of transactions. This creates ethical challenges such as in the case of The DAO where unnoticed weaknesses in the code were used to steal money (Fischer, 2018; Tang et al., 2019a). Smart contracts do not automatically define accountability, so in the event of malfunctioning or violation of contracts, users should have ways of disproving transactions in order to protect their rights (Parkhomenko et al., 2019).

4.7 Inadequate regulation (I7)

Blockchain is still a relatively new technology and legal and regulatory frameworks are not widely in place yet. One of the issues is the absence of customer protections and guarantees found in regular markets (Huang and Zhang, 2019). Additionally, blockchain systems involve ownership of assets, such as fungible and non-fungible tokens, and the same legal regulation and rights should apply for digital records and properties as do for traditional ones (DuPont, 2019; Ehrenberg and King, 2020; Fischer 2018; Migliorini et al. 2019; Parkhomenko et al., 2019; Perdana et al., 2021; Rana et al. 2021). Indeed, ownership of assets could delegate legal rights, obligations, and governance in the blockchain system (Beck et al., 2018). Patents can be used to ensure rights; however, they can also be used as trolling to create disputes or provoke network peers (Drobyazko et al., 2019).

5 Ethical values within the European Union

All countries and societies would do well to reflect on the ethical blockchain issues identified earlier. But to estimate the effects on citizens and society at large, the specific culture and ethical norms of a country must be taken into account. Therefore, it is important to consider various regions' ethical and

cultural values when developing guidelines and to recognize that different regions may have different perspectives. In this paper, we have applied the identified ethical issues in the context of the European Union. In part, we have done so because of the EU's vast amount of available and explicitly defined norms and rules for digital systems. In the context of blockchain, European Commission documents state the importance of having EBSI meet "the highest standards in terms of privacy, cybersecurity, interoperability and energy efficiency, as well as [being] fully compliant EU law" (European Commission, 2018a, p.1). EU values are also mentioned by the CEF, which states that "EBSI will meet the highest standards in terms of privacy, cybersecurity, interoperability, and energy efficiency [and will be] fully compliant with EU law" (European Commission, 2018b, p.1). In the following, we identify seven key European values, using official EU documents and declarations as well as academic literature.

5.1 Human dignity (V1)

The EU Charter of Fundamental Rights states that "the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity" (European Union, 2012, preamble). Human dignity is here described as a "universal value" that forms one of the cornerstones of the European Union and thus something that must run through all the EU's decisions and actions. The charter states that "Human dignity is inviolable. It must be respected and protected" (European Union, 2012, article 1). Human dignity acknowledges all humans as individuals and not mere instruments or objects (Schachter, 1983). In the context of blockchain technology, respect for human dignity encompasses ethical reflections on the needs of the users of blockchain systems and the impacts of those systems. It is imperative that autonomous actors, such as smart contracts, do not gain more authority than human agents, as this risk dehumanizing individuals in their interaction with the technology, and thus violate their intrinsic human dignity.

5.2 Freedom (V2)

Historically, freedom has been discussed in the context of the theological question of whether humans have the freedom of choice (Schachter, 1983). But the European Convention on Human Rights suggests that persons have free will and are endowed with the following rights: "Article 10 freedom of thought, conscience and religion, Article 11 freedom of expression and information, and Article 12 freedom of assembly and association" (European Union, 2012, article 10–12). If the freedom of choice did not exist, there would be no need for protecting these rights. In official EU documents, freedom is treated as something universal that automatically exists, unless it is limited by others. Today, the discussion is less focused on theological issues and more concerned with how algorithms influence our decisions, as well as people's right to freely choose which system to participate in. According to the European Commission, it is important that "algorithms and artificial intelligence are not used to predetermine people's choices, for example regarding health, education, employment, and their private life" (European Commission, 2022, p.4). When it comes to blockchain systems, however, users can only choose among predefined options. In such a scenario, it is not God that limits or influences the freedom of choice, it is developers and code. It is therefore important that blockchain systems be designed to support interoperability and to avoid digital fragmentation, as this could otherwise limit the free movement of people between systems. However, blockchain technology can also support some of the European Union's expressed aims, such as "the right to freedom of expression in the online environment, without fear of being censored or intimidated" (European Commission, 2022, p.5).

5.3 Privacy (V3)

Privacy is a key European value. It is stated in the EU Charter that "Everyone has the right to respect for his or her private and family life, home and communications" (European Union, 2012, article 7). Yet it is difficult to find a single, clear definition of the term "privacy." Solove (2008) suggests that instead of trying to define privacy, one should focus instead on activities that can cause privacy

problems. The EU Charter states that everyone has the right to confidential communication and that no one should be asked to provide more data than necessary when using public services (European Union, 2012, article 8). It furthermore states that everyone should have the right to access data collected concerning themselves, as well as the right to correct that data when it is false. In relation to blockchain systems, two types of privacy issues are particularly likely to arise. The first concerns the correction of incorrect personal data. As blockchain systems have immutable ledgers, it is important that no personal or sensitive data be stored directly on the ledger. The second privacy issue deals with the dissemination of data. As the ledger is distributed among all nodes in a network, it is important that only data that is suitable for network distribution gets stored on the network.

5.4 Justice and fairness (V4)

The Rome Declaration states that the EU is "a Union which promotes equality between women and men as well as rights and equal opportunities for all" (European Commission, 2017). This distribution, or allocation, of rights and opportunities, is known as distributive justice. In relation to digitization, the EU commits to ensuring equal access to digital education and safe online services that support participation in democracy: "Everyone should have access to digital technologies, products and services that are safe, secure, and privacy-protective by design" (European Commission, 2022, p.5). It is therefore important that algorithms and systems be designed and coded to avoid discrimination and exclusion. For digital systems, it is especially important to ensure access for "elderly people, persons with disabilities, or marginalized, vulnerable or disenfranchised people and those who act on their behalf," as these people might get overlooked or fall behind (European Commission, 2022, p.3).

5.5 Transparency (V5)

Reports from the European Union (2012) and European Commission (2022) mention two types of transparency: One is the right to access personal information regarding oneself that is collected, stored, and managed by others. The other is the right to transparent information regarding the systems that one uses. Transparency of personal data is described as "the right of every person to have access to his or her file while respecting the legitimate interests of confidentiality and of professional and business secrecy" (European Union, 2012, article 41). Transparency of systems includes public institutions, private online services, and algorithm transparency. Everyone has the right to access "documents of the institutions, bodies, offices and agencies of the Union, whatever their medium" (European Union, 2012, article 42). Additionally, people have the right to be informed when they are interacting with AI and algorithms (European Commission, 2022). Transparency of relevant information can thereby help ensure accountability, safety, public services, and informed consent (Turilli and Floridi, 2009). However, to avoid the ethical issues around revealing sensitive data, information must be carefully considered in relation to the specific context before it is made transparent (Turilli and Floridi, 2009). This especially applies to data stored in blockchain systems, as the ledger is immutable. However, that same feature can also be used to increase transparency, particularly in public institutions and government processes.

5.6 Safety and security (V6)

Security can be understood in the context of two dimensions: physical and non-physical as well as human-made and non-human-made (King and Murray, 2001). The protection of individual security is directly mentioned in article 5 of the European Convention as the "right to liberty and security" (2013). Article 5 discusses security in the context of arrest and detention and thus centres a physical threat to an individual. However, EU documents also mention non-physical security in the context of "legal, economic and social protection" (European Union, 2012, article 33) as well as in the context of social security and customer protection (European Union, 2012, article 33–34, 38). In the context of technology, it is declared that digital systems should be "safe and used in full respect of people's fundamental rights" (European Commission, 2022, chapter 1). Online forums should be safe and

protected against misinformation, as well as resilient against "cybercrime, including data breaches and cyberattacks. This includes protecting digital identity from identity theft or manipulation" (European Commission, 2022, chapter 5). Security in relation to a blockchain is understood as protection from both physical and non-physical harm, whether it is human-made or not. For blockchain systems security threats include, but are not limited to, hacking, attack on one's person or reputation, misuse of personal data, discrimination by biased systems, and the exclusion from essential online systems and services.

5.7 Societal and environmental well-being (V7)

The European Union supports the UN Sustainable Development Goals (European Commission, 2019b) and aims to be climate-neutral by 2050; it is committed to a "high level of environmental protection and the improvement of the quality of the environment" (European Union, 2012, article 37). The Rome Declaration declares that EU members pledge to work toward a sustainable Europe and a clean and safe environment (European Commission, 2017). In regard to digital transformation, digital solutions should be developed to have a minimal impact on the environment. This includes promoting a "circular economy, [in which] digital products and services should be designed, produced, used, disposed of and recycled in a way that minimizes their negative environmental and social impact" (European Commission, 2022, p.6). Furthermore, digital solutions that have a positive impact on the environment and climate should be developed and deployed. For blockchain, this means designing and employing systems that cause the least possible harm to the environment, as well as developing new blockchain-based solutions that can support sustainable change. Blockchain systems utilizing smart contracts can be designed to calculate, track, and report carbon emissions from transport or entire value chains, which will significantly advance transparency, traceability, and accountability (European Commission, 2021).

6 Ethical guidelines for blockchain systems based on EU values

Since the European Union has not defined ethical guidelines for blockchain technology, we use the blockchain issues listed in section 4 and the EU values listed in section 5 as the foundation for proposing ethical guidelines for blockchain systems (see table 2). Below, we discuss and make ethical recommendations for blockchain systems.

Guidelines	EU values	Ethical issues
1 Security	V1, V6	I5
2 Privacy	V3	I2
3 Equality and Accessibility	V1, V2, V4	I2, I3
4 Societal and Environmental Well-being	V1, V2, V3, V5, V7	I1, I4
5 Accountability	V1, V4, V5	I3, I6
6 Governance	V1, V5, V6	I1, I3

Table 2. Ethical Guidelines Based on EU Values and Ethical Issues.

6.1 Security

It is essential that blockchain systems be designed to ensure the security of the users (V6). We recommend putting people in focus and designing security precautions that ensure the safety of both the network as a whole and the individual nodes and users (V1). A safe and secure system is in the interest of the majority of the network and is vital for the business- and public processes that depend on the

system. We recommend that designers be mindful of system threats (I5) like hijacking, private keys, weak code, and hard forks when designing and developing blockchain systems.

As the ledger in the blockchain system is stored on multiple nodes, the data is protected from manipulation, and the system is robust in the event of the physical breakdown of servers. This supports the EU's commitment to keeping data safe from theft or manipulation. However, a network can be overtaken by malicious nodes, putting the data and the system at risk if more than a certain per cent of the network is attacked or hijacked. We therefore recommend that developers consider the number, ownership, and physical location of nodes when designing blockchain systems. The degree of decentralization will be linked to the level of security required by the system, with more nodes ensuring a higher level of robustness. In a European context, we recommend cross-border blockchain systems, with nodes in more than one EU country. For public solutions like EBSI, we recommend having one or more national nodes in every member state. An additional aspect to be aware of is the risks of private keys, which are unique and cannot be retrieved if lost. Individuals risk losing their digital assets, data, or digital identity if their key (for example, a hard disk) gets lost or stolen. A private key can also be compromised or lost if the computer gets hacked. Hence a secure way for storing private keys (both for users and for systems) must be of the highest priority. We recommend due diligence when deciding where to keep one's private key. We also recommend choosing solutions with modern encryption and updated algorithms, to minimise vulnerabilities and security threats to users and the system. Malicious users can exploit weak code and jeopardize the whole system and all its users, as happened in the case of The DAO scandal. Therefore, we recommend having an audit process before a system is launched and continuously throughout the system's lifecycle to identify any weaknesses that can put it in danger. Finally, hard forks may be the last way of salvaging a system that has been compromised, as a way to "reset the system." We recommend preliminary reflections on when it is ethically responsible to create a hard fork and how to ensure that only one true version of the ledger exists afterwards. When it is possible, we also recommend allowing the stakeholders of the system to participate in the decision on whether to do a hard fork or not.

6.2 Privacy

Blockchain technology creates quasi-immutable data, that data must be accurately, truthfully, and suitably stored, as it is extremely challenging to change. Records of reputation, health information, or other sensitive private data (for example concerning sexual orientation, age, gender, religious or political views) can create harm and unwanted consequences for individuals and companies (V3). Therefore, it is vital when designing blockchain-based systems that no incorrect or inappropriate data be stored in a blockchain system. Additionally, data must be substantiated and of high quality. We identify data privacy (I2), in the context of the immutable ledger and data distribution, as a core concern for system designers.

First, EU regulations such as GDPR affirm that people have the right to access, update and delete personal data, which can be a challenge for data stored in a blockchain system. As blockchain systems become more broadly used, it is important that users understand the risks and consequences of uploading sensitive data to a ledger, as it will be close to impossible to correct or delete once stored. Therefore, we suggest that users get clearly informed about how data is stored and which data to avoid uploading. For systems that do not allow pseudonymous identities, we recommend having safe authentication methods to ensure the identity of new users.

Second, the ledger data gets distributed to all nodes in the network. This creates trust and transparency in the system, as all nodes can check the data stored. However, it also requires that the data be suitable for distribution among many, often unknown, people. Again, we advise clear guidelines for users, to increase their knowledge of the system they are interacting with. In public solutions, we recommend designing and developing systems that protect the user's data by being private-by-design.

6.3 Equity and access

The EU value of justice and fairness (V4) demonstrates that the European Union puts a high regard on ensuring equal access and opportunities for all. However, issues of unintended discrimination, accessibility, or exclusion in blockchain systems are not often mentioned in literature (I2). Even so, the importance of this ethical issue is such that it should be addressed in these guidelines.

The European Union is based on values of human dignity and justice and fairness. However, as blockchain systems are difficult or nearly impossible to change once implemented, the decisions made in the design phase can create unintended, negative consequences for users and society, if not critically assessed before the launch (I3). It is especially important to avoid unintended discrimination or harm caused by public-use blockchain systems (V1). We recommend involving all relevant stakeholders in the design and development phase, to prevent creating biased systems. In addition, we recommend that specific frameworks for developers be created to support them in the development phase and help ensure that blockchain systems are unbiased and reflect social norms and values. Biased systems can be inaccessible for some users. We believe it is important to make accessibility an explicit priority in system design so that the system does not exclude minorities or other marginalized stakeholder groups, including people with limited tech savvy and people who do not have high-performing computers (I2). Systems must be accessible across generations and cultures, as well as for disabled and vulnerable users. We recommend a user test for blockchain systems to ensure that they are designed in a supportive way that includes all stakeholders.

The European Union supports physical and digital freedom of movement (V2). Users' personal data should be accessible and transportable across borders and systems. It is therefore important to create blockchain-based applications that support interoperability with other digital solutions. Blockchain technology can, for example, be used to create interoperable digital identity solutions that allow identity and personal credentials to be verified across Europe. It is important that blockchain solutions be designed to support mobility and not become digital silos. We therefore recommend that European blockchain solutions be designed to be interoperable and to centre the user's freedom of movement. To ensure interoperability, we recommend that blockchain systems be designed using international blockchain standards.

6.4 Societal and environmental well-being

The EU prioritizes societal and environmental sustainability. It is important that the digital transformation protects and supports people, while at the same time sustaining the EU goal of becoming climate neutral by 2050 (V7). We therefore advise that developers designing blockchain systems particularly reflect on supreme power by design (I1) and on the depletion of resources (I4).

Blockchain technology can be used to support sustainable economic development and help fight climate change, which supports the EU goal of becoming energy-neutral by 2050. However, developers must choose which blockchain algorithm to base their system on. Therefore, we suggest that risk assessments be made, to ensure that the right balance between safety and energy consumption is found. When it is responsible and possible, we recommend that energy-efficient consensus mechanisms be selected. We also suggest that blockchain technology be used to support sustainable development in general, for example through carbon emission chain tracking or supply chain transparency. We recommend that precautionary steps be initiated to ensure environmental responsibility at all levels of the supply chain of blockchain systems.

As mentioned earlier, it is possible to design blockchain systems where decision power is not fully decentralized. In such cases, centralized authorities can potentially use blockchain technology to monitor transactions and become even more powerful. Such a surveillance system would be in conflict which EU values, especially the values of human dignity (V1), freedom (V2), privacy (V3) and transparency (V5). It may be beneficial to consider the follow-on effects that blockchain systems have on digital processes, institutions, and governance. We therefore recommend that designers and implementers

conduct social risk assessments as well as technical and economic ones before a blockchain system is adopted.

6.5 Accountability

There are also assorted ethical issues that emerge around accountability, particular when it comes to smart contracts (I3), pseudonymous users (I6), and unauthenticated data (I6). Smart contracts may create unwanted effects that were practically impossible for the developer to foresee. Pseudonymous users can conduct malicious behaviour in a system with little or no risk of prosecution. And incorrect data added to a blockchain system might impede accountability and transparency.

Smart contracts are designed to automatically execute when predefined settings are met. They are not capable of adjusting to a specific situation or reflecting on the validity of the predefined settings or the consequences arising from the execution. This risk dehumanising people as the processing of individual cases is not done with a focus on the individual human but is instead governed by predefined criteria. We therefore recommend developers be mindful of the potential impact on people when defining smart contracts (V1). But even the most careful developers cannot envision all possible situations and impacts when implementing smart contracts. A way to lower the risk of unintended effects from smart contracts (as well as the harm caused by deliberate misuse) is to make the code and process transparent and understandable for laypeople (V5). This will allow multiple people, instead of only a handful of developers, to check the code for bias and other vulnerabilities. We also encourage continued auditing, especially for smart contracts facilitating critical processes in society, to ensure that they uphold the newest regulation. Finally, we suggest giving users a way of appealing unjust or improper execution of smart contracts (V4).

Pseudonymous wallets can cause accountability problems in blockchain systems, as it is hard to place responsibility if the identity of a wallet holder is hidden or not authenticated (V5). This is especially true for blockchain solutions facilitating critical infrastructure, as the consequences of misuse can be more severe for all involved users. Lack of authentication can also cause problems in the context of data. Therefore, it is important to ensure that the data stored in a blockchain system is authentic. We recommend that risk assessments be made in relation to smart contracts, users, and data, to determine when authentication is imperative. For example, it might be helpful to implement a trustworthy audit system for authenticating identity and data before they enter the blockchain system..

6.6 Governance

The governance structure of a blockchain system is defined in the design phase and pre-programmed incentive mechanisms can be hard or impossible to change once the system is launched. It is therefore important that developers reflect on both decision rights (I1) and incentive mechanisms (I3), as well as how these unfold over the life cycle of a blockchain system before it is launched. We recommend that blockchain developers take the entire life cycle of a blockchain system into account, to ensure that the system expresses its central values and goals at every stage.

First, developers distribute decision rights in the system (V1). In blockchain systems, users' decision rights are predefined in the design phase and are difficult to expand or change later. Therefore, we recommend developers be mindful when deciding how to distribute decision rights in the system to not violate EU values. In some cases, a more centralized design might be warranted to ensure security (V6). In other situations, a fully decentralized system will be needed to protect the system from censorship and interference from unwanted authorities (V5). No matter the degree of decentralization, we encourage developers to put people at the centre of their decisions, to ensure that distributed decision rights support the safety and human dignity of people (V1, V6).

Second, in the design phase of a blockchain system, developers can choose the incentive mechanisms that will maintain the system and keep it secure. However, sometimes users do unintended things which create new, unintended incentives, just as happened on the betting platform Augur (I3). Users'

motivations for participating in a system might change along the system's life cycle, and we therefore recommend that developers reflect on avoiding misuse of the system, both in its initial phases and in the event of successful adoption by many users. However, we also advocate using incentives to keep the system stable and secure (V6). Incentive mechanisms can be used to mitigate risks to the network, and a mindful use of incentives is encouraged to keep the network protected. Finally, developers must address all life-cycle stages of a system. Although blockchain systems are based on a principle of decentralization, the developers have centralized decision power in the design phase before a system is launched. To ensure that the system upholds and reflects ethical values, we encourage developers to reflect on all stages of the system's life cycle, from design, implementation, and deployment to possible termination. If a system is terminated, should its data be migrated to another system? And what should be done if a system develops in a way that starts to violate the very principles it is built on? We therefore recommend that developers reflect on the long-term effects of their decisions and acknowledge and be respectful of the centralized decision power they have in the design phase.

7 Limitations and further studies

In our analysis, we focused on EU values, which limits this research from being applied fully in an international context. However, our research creates a foundation for how European and international standards could be developed along with frameworks for developers designing and developing blockchain systems. The findings collected from our literature review reflect the fact that we took an IS point of view, which means that additional issues might have been found if more journals had been included. For instance, based on our understanding of EU values and blockchain technology, we believe that interoperability is an ethical issue; however, it has not been addressed in the literature and did not appear as a finding when we identified ethical issues for blockchain systems. Of the seven ethical issues that were identified in the literature, we did not discuss inadequate regulation (I7), as we consider the issue outside the scope of this paper. However, we do recommend that future studies investigate legal and regulatory frameworks. We recommend that research be conducted to understand this issue in depth. Additionally, we suggest that a blockchain system can be designed in different ways to allow for a more public or private state. It could be valuable for future research to consider these general guidelines in the context of permissioned, permissionless, private, and public blockchain systems.

8 Conclusion

Technology influences how organizations are structured and organized. It provides new ways of processing workflows and connecting people and thus influences how we interact and how we structure society. Blockchain is a disruptive technology with potentially widespread societal consequences across multiple sectors. It is therefore important that blockchain systems be built on ethical values and guidelines that support the morals and beliefs of society. This paper proposes six ethical guidelines for blockchain systems, as well as presents seven ethical issues specific to blockchain technology. These ethical issues have been analysed and discussed in the context of EU values to make recommendations for how blockchain technology can be used to uphold and enforce European principles and values. As blockchain systems are decentralised and immutable, it is hard to change the system once it has been implemented. Therefore, developers must already in the design phase address possible ethical issues arising on a network level, along with ethical issues occurring in later life-cycle stages. However, research conducted on ethics in relation to blockchain technology is currently scarce. We propose, that blockchain systems should embrace ethical norms and values as a part of the system specifications and requirements during the design and implementation phase. The current ethical research in IS focuses on individual behaviour in a specific context, but as blockchain systems are decentralised and network-based, additional research must be conducted. This paper aims to fill in that gap by identifying ethical issues for blockchain technology mentioned in blockchain research. These ethical issues must be addressed to design blockchain systems that implement and protects ethical principles and values.

9 References

Alshamsi, A. and Andras, P. (2019). "User perception of Bitcoin usability and security across novice users," International Journal of Human-Computer Studies (126), pp. 94–110.

Anderson, M. and Anderson, S. L. (2020). "Machine ethics: Creating an ethical intelligent agent," in Machine Ethics and Robot Ethics, Routledge, pp. 237–248.

Ar, I. M., Erol, I., Peker, I., Ozdemir, A. I., Medeni, T. D., and Medeni, I. T. (2020). "Evaluating the Feasibility of blockchain in logistics operations: A decision framework," Expert Systems with Applications (158), p. 113543.

Aydar, M., Cetin, S. C., Ayvaz, S., and Aygun, B. (2019). "Private key encryption and recovery in blockchain," arXiv preprint arXiv:1907.04156 ().

Bamakan, S. M. H., Motavali, A., and Bondarti, A. B. (2020). "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications (), p. 113385.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., and Danezis, G. (2017). "Consensus in the age of blockchains," arXiv preprint arXiv:1711.03936 ().

Beck, R. (2018). "Beyond bitcoin: The rise of blockchain world," Computer (51:2), pp. 54–58.

Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. (2017). Blockchain technology in business and information systems research.

Beck, R., Dibbern, J., and Wiener, M. (2022). "A Multi-Perspective Framework for Research on (Sustainable) Autonomous Systems," Business & information systems engineering (forthcoming).

Beck, R., Müller-Bloch, C., and King, J. L. (2018). "Governance in the blockchain economy: A framework and research agenda," Journal of the Association for Information Systems (19:10), p. 1.

Benke, I., Feine, J., Venable, J. R., and Maedche, A. (2020). "On implementing ethical principles in design science research," AIS Transactions on Human-Computer Interaction (12:4), pp. 206 227.

Calvaresi, D., Calbimonte, J.-P., Dubovitskaya, A., Mattioli, V., Piguet, J.-G., and Schumacher, M. (2019). "The good, the bad, and the ethical implications of bridging blockchain and multi agent systems," Information (10:12), 363.

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., and Arami, M. (2020). "How Blockchain can Impact financial services–The overview, challenges and recommendations from expert interviewees," Technological Forecasting and Social Change (158), p. 120166.

Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., and Sarda, P. (2018). "Blockchain versus database: a critical analysis," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On BigData Science And Engineering (TrustCom/BigDataSE), IEEE, pp. 1348–1353.

Couger, J. D. (1989). Preparing IS students to deal with ethical issues. Mis Quarterly, 211-218.

Dierksmeier, C. and Seele, P. (2018). "Cryptocurrencies and business ethics," Journal of Business Ethics (152:1), pp. 1–14.

Dierksmeier, C. and Seele, P. (2020). "Blockchain and business ethics," Business Ethics: A European Review(29:2), pp. 348–359.

Drobyazko, S., Makedon, V., Zhuravlov, D., Buglak, Y., and Stetsenko, V. (2019). "Ethical, technological and patent aspects of technology blockchain distribution," Journal of Legal, Ethical and Regulatory Issues (22), pp. 1–6.

DuPont, Q. (2019). "Guiding principles for ethical cryptocurrency, blockchain, and DLT research," Blockchain, and DLT Research (July 4, 2019) ().

Ehrenberg, A. J. and King, J. L. (2020). "Blockchain in context," Information Systems Frontiers (22:1), pp. 29–35.

Ertemel, A. V. (2018). "Implications of blockchain technology on marketing," Journal of international trade, logistics and law (4:2), pp. 35–44.

European Commission (2017). "The Rome Declaration," (available online at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_17_767)

(accessed: 16.10.2022).
European Commission (2018a). "European countries join blockchain partnership," (available online at https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership). (accessed: 28.04.2022).
European Commission (2018b). "The European Blockchain Service Infrastructure is on its way," (available online at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/09/25/The+European+Blockchain+Services+Infrastructure+is+on+its+way). (accessed: 28.04.2022).
European Commission (2019a). "Ethics Guidelines for Trustworthy AI, pilot," (available online at https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/pilot-assessment-list-ethics-guidelines-trustworthy-ai). (accessed: 28.04.2022).
European Commission (2019b). "The European Green Deal," (available online at https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0002.02/DOC_1&format=PDF). (accessed: 03.05.2022).
European Commission (2021). "Blockchain for climate action," (available online at https://digital-strategy.ec.europa.eu/en/policies/blockchain-climate-action). (accessed: 28.04.2022).
European Commission (2022). "European Digital Rights and Principles," (available online at https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and principles). (accessed: 28.04.2022).
European Convention (2013). "European Convention on Human Rights," (available online at https://www.echr.coe.int/documents/convention_eng.pdf). (accessed: 28.04.2022).
European Union (2012). "EU Charter of Fundamental Rights C 303/17," (available online at https://fra.europa.eu/en/eu-charter/article/0-preamble). (accessed: 28.04.2022).
Farrugia, S., Ellul, J., and Azzopardi, G. (2020). "Detection of illicit accounts over the Ethereum blockchain," Expert Systems with Applications (150), p. 113318.
Fischer, D. (2018). "Ethical and professional implications of blockchain accounting ledgers," Available at SSRN 3331009.
French, A., Shim, J. P., Risius, M., Larsen, K. R., & Jain, H. (2021). The 4th Industrial Revolution powered by the integration of AI, blockchain, and 5G. Communications of the Association for Information Systems, 49(1), 6.
Friedman, B. and Kahn, P. H. (2002). "Human Values, Ethics, and Design," in. The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications, USA: L. Erlbaum Associates Inc., pp. 1177–1201.
Gianmarco Baldini Maarten Botterman, R. N. M. T. (2016). "Ethical Design in the Internet of Things," English. Science and Engineering Ethics (22), N/A–N/A.
Gomber, P., Kauffman, R. J., Parker, C., and Weber, B. W. (2018). "On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services," Journal of Management Information Systems (35:1), pp. 220–265.
Hacioglu, U., Chlyeh, D., Yilmaz, M. K., Tatoglu, E., and Delen, D. (2021). "Crafting performance-based cryptocurrency mining strategies using a hybrid analytics approach," Decision Support Systems (142), p. 113473.
Hirschheim, R., & Klein, H. K. (1994). Realizing emancipatory principles in information systems development: the case for ETHICS. MIS quarterly, 83-109.
Huang, H. and Zhang, Z. (2019). "Virtual Standard Currency for Approximating Foreign Exchange Rates," International Journal of Electronic Commerce (23:1), pp. 33–62.
Ingold, P. V. and Langer, M. (2021). "Resume= Resume? The effects of blockchain, social media, and Classical resumes on resume fraud and applicant reactions to resumes," Computers in Human Behavior (114), p. 106573.
Ingram Bogusz, C. and Morisse, M. (2018). "How infrastructures anchor open entrepreneurship: The Case of Bitcoin and stigma," Information Systems Journal (28:6), pp. 1176–1212.
Ishmaev, G. (2020). "Sovereignty, privacy, and ethics in blockchain-based identity management systems," Ethics and Information Technology (), pp. 1–14.

Johnson, D. G., & Miller, K. (2004). Computer ethics. Academy & the Internet, 12, 143.
Jørgensen, K. P., & Beck, R. (2022). Universal wallets. Business & Information Systems Engineering, 1-11.
Kaygın, E., Topçuoğlu, E., and Özkes, S. (2018). "Investigating the Bitcoin System and Its Properties within the Scope of Business Ethics," Is Ahlakı Dergisi (11:2), pp. 186–192.
King, G. and Murray, C. J. (2001). "Rethinking human security," Political science quarterly (), pp. 585–610.
Kučera, J. and Bruckner, T. (2019). "Blockchain and ethics: a brief overview of the emerging initiatives," in CEUR Workshop Proceedings, vol. 2443, pp. 129–139.
Lapointe, C. and Fishbane, L. (2019). "The blockchain ethical design framework," Innovations: Technology, Governance, Globalization (12:3-4), pp. 50–71.
Leonard, L. N. and Cronan, T. P. (2001). "Illegal, inappropriate, and unethical behavior in an Information technology context: A study to explain influences," Journal of the Association for Information Systems (1:1), p. 12.
Li, X. and Whinston, A. B. (2020). "Analyzing Cryptocurrencies," Information Systems Frontiers (22:1), pp. 17–22.
Migliorini, S., Gambini, M., Belussi, A., and Combi, C. (2019). "The Blockchain Role in Ethical Data Acquisition and Provisioning." in PIE@ CAiSE,
Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. sage.
Moor, J. H. (1985). "What is computer ethics?," Metaphilosophy (16:4), pp. 266–275.
Moor, J. H. (2020). "The Mature, Importance, and Difficulty of Machine Ethics," in Machine Ethics And Robot Ethics, Routledge, pp. 233–236.
Myers, M. D. and Venable, J. R. (2014). "A set of ethical principles for design science research in Information systems," Information & Management (51:6), pp. 801–809.
Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). "Blockchain," Business & Information Systems Engineering (59:3), pp. 183–187.
Oz, E. (1992). Ethical standards for information systems professionals: A case for a unified code. MIS quarterly, 423-433.
Ølnes, S., Ubacht, J., and Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.
Palas, M. J. U. and Bunduchi, R. (2020). "Exploring interpretations of blockchain's value in healthcare: a multi-stakeholder approach," Information Technology & People.
Parkhomenko, M., Pustovit, J., Ivanenko, D., Denisov, A., and Voinarivskyi, M. (2019). "Digital law and electronic ethics in the formation of society 4.0," Journal of Legal, Ethical and Regulatory Issues (22), pp. 1–6.
Perdana, A., Robb, A., Balachandran, V., and Rohde, F. (2021). "Distributed ledger technology: its evolutionary path and the road ahead," Information & Management (58:3), p. 103316.
Qureshi, A., Garcia-Font, V., Rifa-Pous, H., and Megas, D. (2021). "Collaborative and efficient privacy-preserving critical incident management system," Expert Systems with Applications (163), p. 113727.
Rana, N. P., Dwivedi, Y. K., and Hughes, D. L. (2021). "Analysis of challenges for blockchain adoption within the Indian public sector: an interpretive structural modelling approach," Information Technology & People.
Richardson, S. M., Petter, S., and Carter, M. (2021). "Five ethical issues in the big data analytics age,"
Communications of the Association for Information Systems (1), p. 18
Rossi, M., Mueller-Bloch, C., Thatcher, J. B., and Beck, R. (2019). "Blockchain research in information systems: Current trends and an inclusive future research agenda," Journal of the Association for Information Systems (20:9).
Ryan, G. W. and Bernard, H. R. (2003). "Techniques to identify themes," Field methods (15:1), pp. 85–109.
Schachter, O. (1983). "Human dignity as a normative concept," American Journal of International

Law (77:4), pp. 848–854.
Scholl, H. J. and Bolivar, M. P. R. (2019). "Regulation as both enabler of technology use and global competitive tool: The Gibraltar case," Government Information Quarterly (36:3), pp. 601–613.
Solove, D. J. (2008). "Understanding privacy,".
Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrapu, R. (2019). "Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain," Journal of Management Information Systems (36:1), pp. 37–73.
Tang, Y., Xiong, J., Becerril-Arreola, R., and Iyer, L. (2019a). "Blockchain ethics research: a conceptual model," in Proceedings of the 2019 on Computers and People Research Conference, pp. 43–49.
Tang, Y., Xiong, J., Becerril-Arreola, R., and Iyer, L. (2019b). "Ethics of blockchain," Information Technology & People.
Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C., and Njilla, L. (2017). "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), IEEE, pp. 469–474.
Toufaily, E., Zalan, T., and Dhaou, S. B. (2021). "A framework of blockchain technology adoption: An investigation of challenges and expected value," Information & Management (58:3), p. 103444.
Turilli, M. and Floridi, L. (2009). "The ethics of information transparency," Ethics and Information Technology (11:2), pp. 105–112.
Vakkuri, V. and Abrahamsson, P. (2018). "The key concepts of ethics of artificial intelligence," in 2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC), IEEE, pp. 1–6.
Vial, G. (2019). "Understanding digital transformation: A review and a research agenda," The Journal Of Strategic Information Systems (28:2), pp. 118–144.
Wallach, W., Allen, C., and Smit, I. (2020). "Machine morality: bottom-up and top-down approaches for modelling human moral faculties," in Machine Ethics and Robot Ethics, Routledge, pp. 249–266.
Webster, J. and Watson, R. T. (2002). "Analyzing the past to prepare for the future: Writing a literature review," MIS quarterly (), pp. xiii–xxiii.
Winfield, A. F., Michael, K., Pitt, J., and Evers, V. (2019). "Machine ethics: The design and governance of ethical AI and autonomous systems [scanning the issue]," Proceedings of the IEEE (107:3), pp. 509–517.
Wynn Jr, D. and Williams, C. K. (2012). "Principles for conducting critical realist case study research in information systems," MIS quarterly (), pp. 787–810.
Yin, R. K. (2003). "Design and methods," Case study research (3:9.2)
Zachariadis, M., Hileman, G., and Scott, S. V. (2019). "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services," Information and Organization (29:2), pp. 105–117.